будущего развития сети и учитывать, какие сервера и рабочие станции будут в ней использоватся. К примеру, если сеть построена полностью на базе решений Microsoft, то проще всего использовать Active Directory. В случае же со смешанной сетью (Unix, Windows) лучше использовать одну из свободно распространяемых служб каталогов.

1. *Laura E. Hunter, Robbie Allen* Active Directory Cookbook, 2006. - 532 p.
2. *Tom Jackiewicz* Deploying OpenLDAP, 2007. - 620 p.
3. *Родерик В. Смит.* Сетевые средства Linux. : Пер. с англ. - М. : Издательский дом "Вильямс", 2003. - 672 с.
4. *Олсен, Гэри Л.* Служба Active Directory Windows 2000: разработка и внедрение : Вильямс, 2001. -624 с.

Поступила 11.02.2010р.

УДК 681.3

В.С. Василенко, к.т.н., НАУ, м. Київ

МОДЕЛЬ ЗАГРОЗ В ІНФОРМАЦІЙНИХ МЕРЕЖАХ

Summary: More detailed and perfect model of threats to the informative resources is offered in the distributed computer networks.

В [1-3] на основі досить детального аналізу множини можливих загроз [4-9] наведено приклад та методику побудови їх моделі, що є певним кроком у визначенні сукупності потрібних засобів захисту інформаційних об’єктів відповідної розподіленої обчислювальної мережі (РОМ) та побудові системи захисту. Але запропонована в [3] модель не дає відповіді на питання щодо механізмів реалізації кожної із множини можливих загроз, а отже не дозволяє конкретизувати склад засобів такої системи захисту. Тому нижче запропоновано більш досконалий варіант моделі загроз. В цій моделі, як і в [3] визначені властивості захищеності інформаційних об’єктів, які можуть бути порушеними – конфіденційність (к), цілісність (ц), доступність (д) та якісна оцінка ймовірності здійснення загроз та рівнів збитків (шкоди) по кожному з видів порушень.

Як і в попередніх матеріалах, методика розроблення такої моделі полягає в тому, що в один із стовпчиків таблиці заноситься по можливості повний перелік видів загроз; в наведеному прикладі такий перелік наведено в стовпчику 2. Надалі для кожної із можливих загроз шляхом їх аналізу (можливо і методом експертних оцінок) необхідно визначити:

ймовірність виникнення таких загроз. Як перший крок визначення такої

ймовірності можна використати її якісні оцінки. В таблиці можуть бути наведені якісні оцінки їх ймовірності – неприпустимо висока, дуже висока, висока, значна, середня, низька, знехтувано низька (стовпчик 3);

на порушення яких функціональних властивостей захищеності інформації (стовпчик 4) вона спрямована (порушення конфіденційності – к, цілісності – ц, доступності – д);

можливий (такий, що очікується) рівень шкоди (стовпчик 5). Приклад цієї оцінки наведено також за якісною шкалою (відсутня, низька, середня, висока, неприпустимо висока). Наявність таких оцінок, навіть за якісною шкалою, дозволяє обґрунтувати необхідність забезпечення засобами захисту кожної з властивостей захищеності інформації;

механізми реалізації (можливі шляхи здійснення загроз) (стовпчик 6).

Наявність такої інформації дозволяє побудувати більш предметну загальну модель системи захисту; оцінити значення залишкового ризику, як функцію захищеності по кожній із функціональних властивостей захищеності; визначити структуру системи захисту та її основні компоненти.

Модель загроз в РОМ

№	Вид загроз	Ймовірність	Що порушує	Рівень шкоди	Механізм реалізації
1	2	3	4	5	6
Моніторинг (розвідка) мережі					
1	Розвідка, аналіз трафіка	висока	к, ц, д	відсутня	Перехоплення інформації, що пересилаються у незашифрованому виді в широкомовному середовищі передачі даних, відсутність виділеного каналу зв'язку між об'єктами РОМ.
Несанкціонований доступ до інформаційних ресурсів із РОМ					
1	Підміна (імітація) довіреного об'єкта або суб'єкта РОМ з підробленням мережних адрес тих об'єктів, що атакують	висока	к, ц, д	середній	Фальсифікація (підроблення мережних адрес IP-адреси, повторне відтворення повідомлень при відсутності віртуального каналу, недостатні ідентифікації та автентифікації при наявності віртуального каналу
2	Зміна маршрутизації	неприпуст. висока	к, ц, д	низький	Зміна параметрів маршрутизації і змісту інформації, що передається, внаслідок відсутності контролю за маршрутом повідомлень чи відсутності фільтрації

Модель загроз в РОМ

№	Вид загроз	Ймовірність	Що порушує	Рівень шкоди	Механізм реалізації
1	2	3	4	5	6
					пакетів з невірною адресою
3	Селекція потоку інформації й збереження її	висока	к, ц, д	високий	Використанням недоліків алгоритмів віддаленого пошуку шляхом впровадження в розподілену обчислювальну систему хибних об'єктів (атаки типу "людина в середині").
4	Подолання систем адміністрування доступом до робочих станцій, локальних мереж та захищеного інформаційного об'єкту, заснованих на атрибутах робочих станцій чи засобів управління доступом та маршрутизації (маскування) відповідних мереж – (файрволів, проксі – серверів, маршрутизаторів та т.п.).	висока	к, ц, д	високий	Використання недоліків систем ідентифікації та автентифікації, заснованих на атрибутах користувача (ідентифікатори, паролі, біометричні дані та т. ін.). Недостатні ідентифікації та автентифікації об'єктів РОМ, зокрема адреси відправника
Специфічні загрози інформаційним об'єктам					
1	Подолання криптографічної захищеності інформаційних об'єктів, що перехоплені	низька	к	високий	Використання витоків технічними каналами, вилучення із мережі та специфічних вірусних атак шляхом впровадження програм-шпигунів (spyware) із розкриттям ключових наборів
2	Подолання криптографічної захищеності інформаційних об'єктів робочих станцій	низька	к	високий	Несанкціонований доступ до інформаційних об'єктів із використанням недоліків систем ідентифікації та автентифікації, заснованих на атрибутах користувача (ідентифікатори, паролі, біометричні дані та т. ін.)

Модель загроз в РОМ

№	Вид загроз	Ймовірність	Що порушує	Рівень шкоди	Механізм реалізації
1	2	3	4	5	6
					із розкриттям ключових наборів
3	Модифікація переданих даних, даних чи програмного коду, що зберігаються в елементах обчислювальних систем.	висока	ц, д	високий	Модифікація чи підміна інформаційних об'єктів (програмних кодів) чи їх частин шляхом впровадження руйнуючих програмних засобів чи зміни логіки роботи програмного файлу із використанням спеціальних типів вірусних атак, спроможних здійснити те чи інше порушення цілісності
					Викривлення певної кількості символів інформаційного об'єкту із використанням спеціальних впливів на інформацію технічними каналами в локальній мережі чи в елементах розподіленої мережі
4	Блокування сервісу чи перевантаження запитами системи управління доступом (відмова в обслуговуванні)	висока	д	високий	Використання атак типу "спрямований шторм" (Syn Flood), передачі на об'єкт, що атакується, не коректних, спеціально підібраних запитів
					Використання анонімних (чи із модифікованими адресами) запитів на обслуговування типу електронної пошти (spam) чи вірусних атак спеціального типу

Слід врахувати, що наведені оцінки ймовірностей та величини можливої шкоди кожної із загроз в даному прикладі моделі загроз носять ілюстративний характер. Для випадків конкретних РОМ ці величини повинні бути визначеними фахівцями служби захисту відповідного підприємства за окремими методиками.

Таким чином, запропоновані в статті аналіз множини можливих типових віддалених загроз в розподілених мережах та механізмів їх реалізації дають можливість визначити складові політики безпеки інформаційних об'єктів

відповідної РОМ та сукупність потрібних засобів захисту від інформаційних об'єктів від можливих загроз із середовища РОМ.

1. *Василенко В.С.* Класифікація та моделювання загроз в розподілених мережах. // К.: Моделювання та інформаційні технології. Збірка наукових праць ІПМЕ ім. Г.Є. Пухова НАН України. - К.: ІПМЕ, 2007. – Вип.. 39 – С. 98– 103.
2. *Василенко В.С.* Оцінка та моделювання загроз в розподілених мережах. Загрози селекції та модифікації інформації. // К.: Моделювання та інформаційні технології. Збірка наукових праць ІПМЕ ім. Г.Є. Пухова НАН України. - К.: ІПМЕ, 2007. – Вип.. 40 – С. 142 – 146.
3. *Василенко В.С.* Оцінка та моделювання загроз в розподілених мережах. Типові атаки в розподілених мережах. // К.: Моделювання та інформаційні технології. Збірка наукових праць ІПМЕ ім. Г.Є. Пухова НАН України. - К.: ІПМЕ, 2007. – Вип.. 40 – С. 108 – 115.
4. TCP під прицілом (http://www.hackzone. ru/articles/tcp.html);
5. Деякі проблеми FTP (http://www. hackzone.ru /articles/ftp.html);
6. Атака на DNS або нічний кошмар мережного адміністратора (http://www.hackzone.ru/articles/dn s−poison.html);
7. *Медведовский И.Д. Семьянов П.В. Леонов Д.Г.* "Атака на Інтернет" М.: Видавництво ДВК 1999;
8. *Соболев К.И.* Дослідження системи безпеки з Windows NT 4.0 HackZone: Територія злому. № 1−2, 1998.
9. Переповнення буфера в WIN32 (http://www.void.ru/stat/9907/20.html).
10. Теорія й практика атак FORMAT STRING http://www.void.ru/stat/0102/27.html+http://www.void. ru/stat/0102/28.html);
11. Перехоплення пакетів TCP: Захист від флуда (http://www.void. ru/stat/9907/19.html).

Поступила 25.02.2010р.

УДК 681

С. М. Головань, А.М. Давиденко, Л.М. Щербак

КОНЦЕПЦІЯ ЕКСПЕРТИЗИ У СФЕРІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

It is shown in work, that conception of examination of defence of information with the limited access is based on the results of analysis of examination on the objects of informative activity, it is suggested to examine in the sphere of information with the limited access in three stages.

Вступ

Захист інформації з обмеженим доступом в інформаційних системах, мережах, приміщеннях, інженерно-технічних спорудах є невід'ємною

